CLAIMS

What is claimed is:

1. A portable device comprising:

a microprocessor; and

a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to a restricted resource, the restricted resource having a communication port communicatively coupled to the portable device, is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the restricted resource is denied to the user otherwise.

2. The portable device as recited in Claim 1 wherein the biometrics-based authentication module is a fingerprint authentication module.

3. The portable device as recited in Claim 1 which is communicatively coupled to the communication port of the restricted resource via a universal serial bus (USB).

4. The portable device as recited in Claim 1 wherein the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the portable device.

5. The portable device as recited in Claim 1 further comprising a non-volatile memory capable or storing biometrics information usable for authentication.

6. The portable device as recited in Claim 1 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.

7. The portable device as recited in Claim 1 wherein the restricted resource comprises a host computer.

8. The portable device as recited in Claim 1 wherein the restricted resource comprises a communication network.

9. The portable device as recited in Claim 1 wherein the restricted resource is a real estate premises that imposes access restrictions.

10. The portable device as recited in Claim 1 wherein the restricted resource is an operable machinery, the safe operation of which requires training.

11. A biometrics-based access control system for controlling access to a restricted resource, comprising:

a portable device which includes a non-volatile memory and a biometrics-based authentication module coupled thereto, wherein the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3) capture a second biometrics marker; and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker, and wherein access to the restricted resource is granted upon a determination of successful authentication and wherein access to the restricted resource is denied otherwise.

12. The biometrics-based access control system as recited in Claim 11 wherein the biometrics-based authentication module is a fingerprint authentication module.

13. The biometrics-based access control system as recited in Claim 11 wherein the portable device is communicatively coupled to a communication port of the restricted resource via a universal serial bus (USB).

14. The biometrics-based access control system as recited in Claim 11 wherein the biometrics-based authentication module comprises a biometrics sensor which is structurally integrated with the portable device in a unitary construction, the biometrics sensor being disposed on one surface of the portable device.

15. The biometrics-based access control system as recited in Claim 11 wherein the non-volatile memory of the portable device comprises flash memory.

16. The biometrics-based access control system as recited in Claim 11 wherein a bypass mechanism for authentication is provided upon a determination of authentication failure by the biometrics-based authentication module.

17. A biometrics-based access control method for controlling access to a restricted resource and implemented using a portable device, the method comprising the steps of:

(a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device;

(b) retrieving a registered biometrics marker from a memory of the portable device, the registered biometrics marker having been stored therein during a registration process;

(c) comparing the first biometrics marker against the registered biometrics marker; and

(d) granting the user access to the restricted resource provided that a match is identified in said step (c).

18. The biometrics-based access control method as recited in Claim 17 wherein the registered biometrics marker is a fingerprint.

19. The biometrics-based access control method as recited in Claim 17 wherein the registered biometrics marker is stored in an encrypted format.

20. The biometrics-based access control method as recited in Claim 17 further comprising the step of denying the user access to the restricted resource provided that a match is not identified in said step (c).

21. The biometrics-based access control method as recited in Claim 17 further comprising the step of providing the user with a bypass authentication procedure provided that a match is not identified in said step (c).